A Cloud-Based Mobile Computing Applications Platform for First Responders

Chit Chung, Dennis Egan, and Ashish Jain
Applied Communication Sciences
Basking Ridge, NJ
ajain@appcomsci.com

Nicholas Caruso and Colin Misner
US Army TARDEC
Warren, MI
colin.m.misner.civ@mail.mil

Richard Wallace
Center for Automotive Research
Ann Arbor, MI
rwallace@cargroup.org

Abstract. **A cloud-based Mobile Computing Applications Platform (MCAP) for enhanced situational awareness and mobile command and control for first responders is introduced. MCAP is a cloud-enabled platform for defining, developing, and deploying apps on smartphones, tablets, and in-vehicle computers. Unique differentiators of the approach include the use of COTS technologies for mobile computing and wireless networking to create a low-cost and sustainable program. A platform architecture that exposes a set of reusable mobile core services that fosters an eco-system of partners to develop feature-rich and innovative apps is discussed. Core services provide support for location, user profile, notification, authentication, content management, and device management. A public-private collaboration and governance model, an essential element for a healthy eco-system, is outlined. The current status of the MCAP program is presented, including experiences from user trials with several Michigan National Guard units.**

Keywords- first responder mobile apps; mobile apps eco-system; core services; mobile command and control; situational awareness; smartphones; cloud based delivery

I. Introduction

First responders currently rely on traditional, two-way radios on public safety bands to provide critical incident related information to operations centers and also for command and control communications. While the need to upgrade to systems that can communicate both voice and data is widely recognized, a cost-effective solution that interfaces with legacy radios and is open and interoperable by design is still missing. This stands in stark contrast to the mobile computing and communications capabilities now possible due to ever progressing commercial wireless broadband networks, smart hand-held devices, portable tablet computers, and on-demand access to cloud services. Further, consumer systems and devices are not only more capable, they are also at least an order of magnitude less expensive.

We developed a cloud-based Mobile Computing Applications Platform (MCAP) to enable a novel approach for defining, developing, and deploying new capabilities for enhanced situational awareness and mobile command, control, communications, and computing (C4). The principal goal of MCAP is to establish an enhanced, interoperable communications capability for homeland defense and civil support responders that embraces the potential that is inherent in modern consumer and commercial wireless communication and computing systems. MCAP relies on an open and collaborative process that leverages Commercial/Government Off-The-Shelf (C/G OTS) systems to rapidly and cost-effectively deliver new capabilities. A key element of our approach is the platform architecture that exposes a set of core services to foster an eco-system of partners to develop feature-rich and innovative applications for first responders. The core services are enablers for interoperability of various applications developed using the platform. The core services detailed in this paper include a Location, Presence, and Availability Service; a Device Management Service; an Authentication Authorization and Access Control Service; a Notification and Messaging Service; and a User Profile and Directory Service. To further streamline rapid delivery of new capabilities, the core services are provided via cloud servers that gracefully scale from very small to large deployments and provide support for different instances for different administrative domains. This cloud-based hosting and delivery model is essential to the business case for creating a sustainable eco-system in the fragmented first-responder marketplace.

In addition to the technical architecture, we also describe a public-private governance model that is critical for creating and sustaining the eco-system of responders, suppliers, and application developers. Indeed, the model is analogous to a commercial App Marketplace model. We demonstrate the technical feasibility of our approach using applications that were developed on the platform for improving situational awareness and mobile C4. In addition to applications developed under the MCAP Program, we also highlight how several COTS mobile apps (e.g., file sharing, collaboration, emergency information lookup, and navigation) were readily adopted into the MCAP suite with user training and well-specified methods and procedures. The ability to tap into the wider commercial Apps Marketplace demonstrates the viability and sustainability of our approach.

This material is based upon work supported by the US Army TACOM under Contract W56HZV-11-C-0365.

UNCLASSIFIED: Distribution Statement A. Approved for public release.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **15 JAN 2013**	2. REPORT TYPE **Journal Article**	3. DATES COVERED **21-02-2012 to 04-01-2013**

4. TITLE AND SUBTITLE **A Cloud-Based Mobile Computing Applications Platform for First Responders**	5a. CONTRACT NUMBER **W56HZV-11-C-0365**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Nicholas Caruso; Colin Misner; Richard Wallace; Chit Chung; Dennis Egan**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Applied Communication Sciences,150 Mount Airy Road,Basking Ridge,NJ,07920**	8. PERFORMING ORGANIZATION REPORT NUMBER **; #23605**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) **U.S. Army TARDEC, 6501 East Eleven Mile Rd, Warren, Mi, 48397-5000**	10. SPONSOR/MONITOR’S ACRONYM(S) **TARDEC**
	11. SPONSOR/MONITOR’S REPORT NUMBER(S) **#23605**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A cloud-based Mobile Computing Applications Platform (MCAP) for enhanced situational awareness and mobile command and control for first responders is introduced. MCAP is a cloud-enabled platform for defining, developing, and deploying apps on smartphones, tablets, and in-vehicle computers. Unique differentiators of the approach include the use of COTS technologies for mobile computing and wireless networking to create a low-cost and sustainable program. A platform architecture that exposes a set of reusable mobile core services that fosters an eco-system of partners to develop featurerich and innovative apps is discussed. Core services provide support for location, user profile, notification, authentication, content management, and device management. A public-private collaboration and governance model, an essential element for a healthy eco-system, is outlined. The current status of the MCAP program is presented, including experiences from user trials with several Michigan National Guard units.

15. SUBJECT TERMS

first responder mobile apps; mobile apps eco-system; core services; mobile command and control; situational awareness; smartphones; cloud based delivery

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Public Release**	**6**	

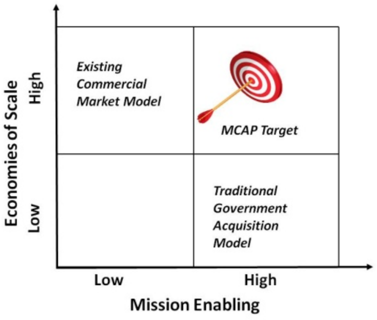
Our system is currently being evaluated by several Michigan National Guard units in their drills and joint training exercises. We provide highlights of these trials and summarize our experiences.

II. Background

A. Objective

The MCAP program began with a 6-month joint study sponsored by the US ARMY TARDEC (Tank Automotive Research, Development and Engineering Center) and the Michigan National Guard to create a Concept of Operations (CONOPS) for a mobile computing application platform that would leverage advances in consumer mobile and cloud computing, vehicular telematics, and cellular networking for supporting joint operations of agencies involved in emergency responses. The goal of the program was to develop a vehicle-centric and highly mobile system that was low-cost, sustainable, and open and interoperable with other incident management systems.

Single-sourced and purpose-built applications are slow to evolve, don't leverage advances in the commercial marketplace in a timely manner, and have high procurement costs. On the other hand, commercial mobile communications and device technologies are rapidly advancing and enjoy tremendous economies of scale. Furthermore, these commercial capabilities appear close to the operational needs of first responders as they enable enhanced situational awareness such as real-time location; provide enhanced mobile communications including voice, video, and text; provide real time asynchronous incident alerts; and facilitate access to operational data and back-end systems from the field. Realizing this inherent dichotomy, The MCAP investigating team set out to define the requirements for a platform and a program that would bridge the gap. The matrix figure above succinctly captures this overarching MCAP objective.


Existing Commercial Market Model
MCAP Target
Traditional Government Acquisition Model
Economies of Scale
High
Low
Low
High
Mission Enabling

B. Functional Requirements

To get a good understanding of technical requirements for MCAP, the team first studied several operational scenarios. The team also investigated the After Action Reports (AARs) from some of the training exercises corresponding to these scenarios. At the end, the following sources were specifically examined:

1. *Michigan National Guard Operational Scenarios*: Because the Michigan National Guard is currently the primary MCAP stakeholder, five operational scenarios relevant to Michigan National Guard were first examined. Michigan has several unique attributes from the Homeland Security perspective including a large international border with three major freight crossing points, a large coastline, and the presence of three nuclear plants. A good example is the operational scenario called "Operation Safeguard" that focused on regional and cross-functional CBRNE readiness and response. The scenario involved terrorist activity and loss of power at a nuclear power plant, train derailment and IEDs and rail yard, coordinated anthrax outbreak, chlorine gas leak, dirty bomb threat at a hospital, and mass evacuation.

2. *National Planning Scenarios:* Another set of considerations that drove the requirements were the National Planning Scenarios [1]. These are a set of 15 all-hazards planning scenarios developed by the Homeland Security Council (HSC) in partnership with the Department of Homeland Security. These high consequence scenarios represent threats or hazards of national significance.

3. *Department of Defense Overseas Contingency Operations:* DoD now emphasizes peacekeeping, nation-building, humanitarian assistance/disaster response (HA/DR), and stability security, transition, and reconstruction (SSTR) missions as much as it does traditional combat missions [2]. Specific to this, DARPA workshop proceedings [3] were consulted to understand the broad requirements for MCAP for assembling the pieces for a Common Operating Picture from a fragmented or even absent networked resources and from NGO organizations with minimal Information and Communication Technology infrastructure.

The above sources resulted in broad functional requirements for mission enabling apps for MCAP, and these are categorized into the following four areas:

1. *Requirements for Developing and Sharing a Common Operational Picture (COP)*

   (a) Real-Time Map Updates: A COP may include several information elements such as status of people, events, weather, assets, buildings, roads, supplies, etc. An important means of presenting this information is to display it on maps with real-time updates. One particular status that is quite important is the geo-location of mobiles and fixed assets.

   (b) Integrated Incident Management: Various software systems and applications are used by first responder organizations to track the progress of an incident, log various decisions and events with time stamps, keep track of assets and supplies, etc. Responders also need to share incident information appropriately, and this requires analysis, transformation, filtering, collation, and policy-based information dissemination. Capabilities such as integration with Unified Incident Command and Decision Support [4] (UICDS), a middleware developed with DHS funding that uses standard compliant schemas to exchange incident information based upon sharing agreements, would be useful.

   (c) Multi-media Content Management: An important element of COP is multimedia content that is generated during an incident. This includes pictures, videos, live video streams, input from vehicle diagnostics, and air quality monitoring and a variety of other sensor feeds.

Effective management, including indexing, adaptation, and cataloging, is required.

2. *Requirements for Establishing Command, Control, Communications and Computing (C4)*

   (a) Portable and Mobile Ad Hoc Networking (MANET): The strongest indication of a requirement for Portable and/or MANETs in support of establishing C4 was demonstrated in an exercise for which the Michigan National Guard had to provide convoy security. Portable networking here means rapid deployment (within a couple hours) of WLAN and backhaul networking using portable communication equipment including Wi-Fi extenders, portable cell-towers, and open spectrum based cellular/satellite bridges. In the convoy use case, a portable network or MANET may be required for the elements of the convoy to remain in constant communication, to generate continuous location updates, and to receive continually updated COP information. Since the Michigan National Guard relies heavily on vehicles to carry out its mission to support first responders, portable networks or MANETs will be necessary to improve the likelihood of vehicles maintaining connectivity to the network and the "cloud."

   (b) Unified Communication (Voice, Video, and Data): Unified communications refers to the ability to integrate a variety of communication modes (SMS, voicemail, email, video, etc.) and making them available through a single interface. Unified messaging is essential to improve the efficiency of accessing communications no matter what mode the sender used. User profiling is another complementing capability that is needed to enable unified communication. User profiles establish identity and other parameters for establishing communications.

3. *Requirements for Securing the Incident Perimeter*

   (a) Credential Checking: The National Guard is often called upon to monitor who gets into the scene of an incident and allow into a secured area only those personnel who need to be there. To aid in identifying people at a secured site, interfaces to credential checking capabilities are required. Such systems may scan a person's badge or identification card and look up attributes of the person in a local database. Such systems are also likely to use biometric identification (e.g., fingerprints and retinal scans), and may need to access a set of remote federated personnel databases maintained and updated by various first responder agencies, military units, and other organizations.

   (b) Video Monitoring, Streaming, and Analysis: This requires the ability to integrate live video feeds from video sensors that keep a watchful eye on the perimeter. While clearly this capability is also needed for assembling the COP, analytics is of particular importance for assisting responders in identification of perimeter breaches. Video analytics clearly has need beyond securing perimeter such as facial recognition and automated damage assessment.

4. *Requirements for Enabling Readiness for Infrequent High-Impact Events*

   (a) Scenario-Driven Application Packs: One means of dealing with the problem of preparing for very infrequent but high impact events is to develop scenario-specific packs of apps. These apps could be made very easily accessible by grouping pointers to the apps along with corresponding procedures and providing "over-the-air" support to push or download them from the cloud. These app packs could reduce the time taken to decide which applications are applicable to a given incident and to find, download, and install them.

   (b) Embedded Training: The second technical requirement enabling readiness for infrequent high-impact events is to make simulated exercise training and multi-media user guides readily accessible for the users. Smartphones and Tablets are ideally suitable for providing such online embedded training. This takes for granted that the apps themselves are easy to use, an expectation increasingly being met by improved and responsive touch user interface on devices.

C. Functional Vision

The MCAP vision is to realize the above functional requirements using an eco-system of app developers. The hallmark of our approach is that we would tap in the creative ability of developers-at-large so that innovation can foster, yet at the same time, provide good governance and certification support so that security and mission enabling requirements are not compromised. This is in sharp contrast to existing approaches to Incident Management with monolithic application stacks that are not easily adaptable for the mobile devices and suffer from heavy system integration burden in making them interoperate. Furthermore, current Incident Management Systems are simply not ready to deal with mobility and mobile computing.

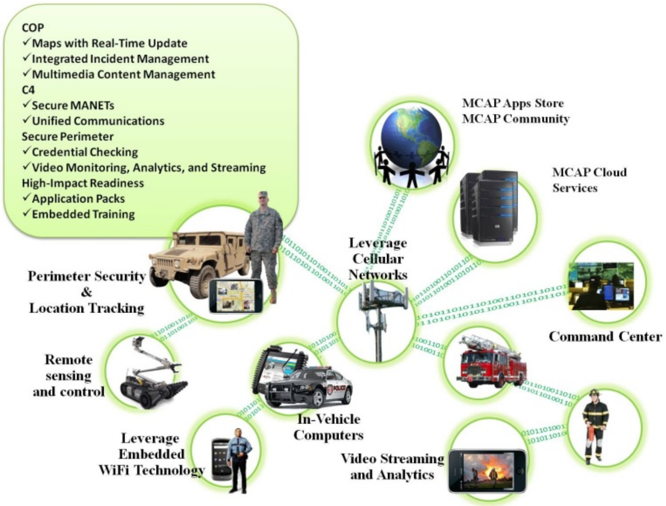

COP
✓Maps with Real-Time Update
✓Integrated Incident Management
✓Multimedia Content Management
C4
✓Secure MANETs
✓Unified Communications
Secure Perimeter
✓Credential Checking
✓Video Monitoring, Analytics, and Streaming
High-Impact Readiness
✓Application Packs
✓Embedded Training
MCAP Apps Store
MCAP Community
MCAP Cloud Services
Leverage Cellular Networks
Perimeter Security & Location Tracking
Command Center
Remote sensing and control
In-Vehicle Computers
Leverage Embedded WiFi Technology
Video Streaming and Analytics

Figure 1 MCAP Functional Vision

III. Platform Architecture

Three requirements are essential to the realization of the functional vision of MCAP shown in Figure 1; these are:

1. Enable a healthy ***eco-system of application providers*** where providers will be able to fully leverage the capabilities of applications and core services already developed
2. Enable a ***public-private governance model*** that will make it easier for new application developers or organizations to join the eco-system and develop new services
3. Enable an ***execution environment*** that is reliable and that scales gracefully from small to large deployments

This section presents the high level platform architecture and provides functional and high level design details for some of its components.

A. Platform Architecture

The MCAP architecture is illustrated in Figure 2, showing a hierarchy of logical tiers. The platform and our approach can be best understood in terms of the value-add of each of the tiers.

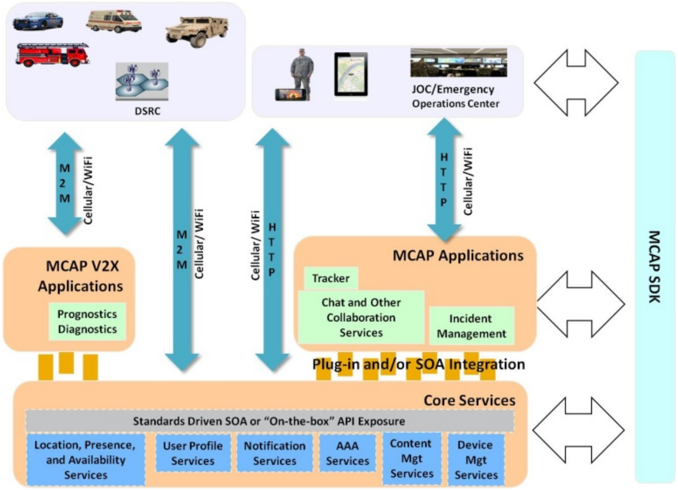


Figure 2 MCAP Architecture

MCAP Core Services software components are shown in the bottom tier and they are provided as Software-as-a-Service via a secure and reliable mobile cloud. Core services include: Location, Presence and Availability; User Profile; Notification; Authentication, Authorization, and Accounting; Content Management; and Device Management. This is the fundamental tier of the Apps Software stack that MCAP proposes to define and make it available to the apps developer community. Each core service is discussed in greater detail in the next section.

The *MCAP Applications* middle tier consists of server-side software components, if any, of MCAP partner applications that will be developed and deployed to meet the MCAP end-users' operational needs. These applications are expected to make heavy use of MCAP core services. The server side component model has to be well-defined so that MCAP application cloud and the MCAP governance processes can manage the software application lifecycle of these components. Our initial goal is to support Web Application Archive (WAR) deployment for web-applications developed by the eco-system partners.

The MCAP program has identified and developed two proof-of-concept applications: *Tracker,* which is an application for Location Tracking with Map Display, and a *Commander's Console,* which is a web-based portal for mobile command and control of incidents that interfaces with COTS Incident Management systems using the UICDS middleware. The MCAP program is also evaluating COTS applications for chat and collaboration and for Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications so that they can be included in the MCAP suite. (Note that applications shown in the figure are illustrative and do not represent a definitive list.)

The *User Interface* top tier consists of the client-side software that executes on hand-held devices and commercial smartphones such as Apple iPhone™, Android phones, or tablet computers such as Apple iPad™. This tier consists of commercial mobile software development platforms provided by the commercial vendors. The MCAP application suite imposes very minimal additional limitations on top of the current frameworks and design principles for mobile applications. A good example of lightweight governance is the client-side composition - a term used for the ability of one independently developed app to be invoked by another independently developed app. To enable client side composition, the MCAP app certification process may require adherence to certain external interface guidelines.

An *MCAP Software Development Toolkit (SDK)* will be provided to all the organizations or individuals who desire to follow the governance framework and develop applications for MCAP. The MCAP SDK will provide an Integrated Development Environment (IDE) for developing new applications. The SDK will be configurable to include some or all of existing MCAP core services and MCAP applications for reuse. This will be cleanly achieved by using a plug-in architecture framework such as OSGi [5].

B. Core Services

MCAP cloud-based core services are the fundamental building blocks for use by other applications and serve the following purpose:

- Provide application developers a uniform mechanism to access certain data such as location information, user preferences, and security and access determination policies
- Allow independently developed applications to use certain common services to increase integration and usability
- Enforce design guidelines

Each core service provides interfaces based upon open protocols and industry standards. Our initial version of the core services employs HTTP(S)/REST interfaces.

Location, Presence, and Availability: Location, Presence and Availability information of MCAP users is critical information for enabling several situational awareness applications. Initial implementation of this core service is mostly based upon the OpenLS [6] industry standard. Location refers to geo-coordinates of a person, feature, or an asset. In addition to the current location, location information history also needs to be preserved. Location information and historical information tracking are very mission and equipment sensitive and thus this core service should be flexible to accommodate several mission-specific requirements for reporting and accessing location information. Presence refers to a user's current access device. This information is vital for other applications to initiate communication requests or send notification messages. Availability information gives an indication about user's current status for accepting communication or messaging requests from other users or applications.

Authentication, Authorization, and Accounting (AAA): In the MCAP eco-system several secure applications would be developed and it is highly desirable that AAA services be logically centralized for all the eco-system partners for both management and usability purposes. Authentication function involves establishing a client's identity using digital credentials and secure communication protocols. Authorization function involves providing access to computational resources after the establishment of the identity. Accounting involves tracking of resource usages for the purpose of auditing, billing, and network management.

The MCAP program plans to maintain a logically centralized copy of the credentials for authentication, policies for access control and authorization, and data for accounting. Our initial approach will be based upon OpenID [7] and OAuth [8].

Notification: Mobile applications are inherently asynchronous and event-driven so apps need the ability to asynchronously send and receive notifications from other applications. Sending, receiving and processing notification across multiple platforms has several inter-operability hurdles. For the MCAP program to evolve such that different devices can be supported, a notification federation service that would provide abstraction to application developers is required. The federation API should provide the adaptors and plug-ins to accommodate multiple device types. The scope of this core service includes messaging, both SMS/MMS and Email, which are specific instances of user-to-user notifications.

User Profile Management: MCAP users need an ability to provide application independent preferences with the expectations that all MCAP application use these preferences for delivering their respective functionalities. This is important for usability. In addition to user preferences, the user profile server should also contain directory information including contact and organization information.

The MCAP eco-system will make use of this information by bootstrapping contact databases on mobile devices and applications such as tracking; and voice, video and text communication applications.

Device Management: Device Management functionality is required for administration and over-the-air support for application deployment and management. Device Management functionality includes the capability to provision organization and application specific profile on devices, send notifications with embedded links for platform and application software updates, locate devices, lockout and wipe device data, and remotely initialize or re-initialize devices. The MCAP program plans to use a COTS device management solution and is in discussion with leading vendors of Device Management services.

Multi-Media Content Manager: Improving situational awareness using multi-media content is going to result in a lot of digital content which needs to be stored and managed. The eco-system partners can also exploit this content to create useful visualization apps such as slide shows and 'heat' maps. Once again, MCAP will use a COTS content server that would allow efficient indexing, searching, tagging, and content adaptation to fit the streaming needs of apps. The MCAP investigating team is currently evaluating several open source content servers for an initial implementation of this service.

IV. MCAP Governance

The MCAP program will be a vehicle of public-private partnership that should enable good returns for all the members in the value chain. MCAP governance serves four goals: (1) help identify key customer needs, (2) govern the technical and business roadmap of the core platform with common capabilities for reuse by commercial partners, (3) enable a healthy ecosystem of commercial partners that can address customer needs, and (4) enforce Service Level Agreements so that services can be provided reliably.

To meet the first goal, the MCAP program plans to have a formal process to manage and prioritize key customer requirements. The process will proactively seek customer inputs which is a role that is very analogous to product management in a commercial organization. This stage may also involve creating rapid proof-of-concept capability demonstrations to validate customer requirements. The principal goal of the MCAP system is to support on-the-go, real-time, and secure access to data and applications for first responders. Therefore, the program would become an important vehicle for collection and prioritization of first responder requirements.

The second goal can be best achieved using a public-private governance structure in which the key customers and suppliers are part of the governance board. With this structure in place, the key commercial partners will have an active role and voice in setting both the technical and business roadmap for the ongoing development of MCAP. The MCAP program is currently evaluating several best practices in creating such partnership and governance boards.

For the third goal of creating a healthy eco-system of commercial partners, it is important that there are real economic profits for the partners. There are at least three means to achieve this. First, the MCAP platform should largely rely on commercial components which have both government and non-government usage–especially for the components related to mobile computing. This could result in amortization of per license costs. Secondly, the MCAP program will provide partners easy access to an array of customers and other core assets such as centralized location and user profile directories for creating new innovative applications. Finally, the governance structure should be such that while government entities at various levels shall retain influence on roadmap, the board should ensure a marketplace-based approach for technology adoption and value distribution.

The fourth goal of MCAP project management is the enforcing of Service Level Agreements (SLAs) between partners and MCAP customers. Project management should have a formal process for defining and evaluating SLAs. The MCAP program, on behalf of its supported customers, should be the vehicle for managing those SLAs.

V. MCAP User Trials

MCAP, with proof-of-concept platform and services, is currently implemented and being evaluated by several units of the Michigan National Guard. In addition to *Tracker* and *Commander's Console*, the MCAP app suite includes several COTS apps that provide desired functionality, even without any integration with MCAP core services, and these are provided as part of the MCAP suite. These apps provide: (a) Cloud-based storage solution that allows sharing of files; (b) Mobile capability to use Defense Connect Online (DCO); (c) Ability to complete PDF forms on smartphones; (d) Video streaming and one-to-many sharing of video streams; (e) Ability to record routes and waypoints and share them with others; (f) Offline guide and source of information on home, office, and industrial chemical compounds; and (g) Ability to obtain real-time weather information.

Our training and trials have been with three Michigan National Guard units, the 51st Civil Support Team (CST), the Counter Drug Team (CDT), and the Joint Staff (J-Staff). The CST exercises included up to 12 soldiers involved in air-quality monitoring and CBRNE threat identification and mitigation scenarios. The CDT scenarios involved combinations of several soldiers deployed on foot in heavily wooded rural areas combined with airborne observers assisting local law enforcement officials monitoring and reporting on suspects' locations, movements, and possession of illegal drugs. The J-Staff Operation simulated numerous terrorist threats over several weeks' time by delivering scripted "inserts" or warnings describing threats to be investigated and mitigated. The J-Staff scenarios required coordination with the Joint Operations Center (JOC), local law enforcement, and reports from Liaison Officers (LNOs) positioned at incident sites and Emergency Operations Centers (EOCs). The MCAP investigating team provided initial training and provisioned the members with iPhones and commanders with iPads. CDT team members were already equipped with iPhones and MCAP team provided links for Over-the-Air (OTA) provisioning of MCAP Apps.

The MCAP investigating team participated in debriefings, "hot washes," and feedback sessions following the exercises. The team elicited feedback regarding training effectiveness, MCAP functionality, the pros and cons of different devices and networks that were trialed, and suggested changes. The handheld smartphones and apps have been generally very well received and found to be useful in the field to support the National Guard missions. Among the most useful functions identified were (a) cellular voice communication, SMS, and email where radio communication was not possible, (b) sharing pictures and video taken from a remote site, (c) semi-automated form filling using smartphones and tablets, and (d) communication and training sessions using Defense Connect Online. Somewhat surprisingly, soldiers typically preferred to use the tablets instead of the smartphones. The tablets' larger screen size and easier data entry overcame any issues related to their greater size and weight. Suggested improvements included better structured and (for some) slower-paced training on the apps (and faster-paced for others), methods to improve battery life especially for location tracking apps, and more useful and usable in-vehicle computers. Tests to date suggest that the most effective in-vehicle computer and communication device might be a handheld tablet.

We participated in a joint emergency preparedness exercise in October 2012 involving over 100 emergency first responders from 15 local, county, state, and federal agencies. A major goal of the exercise was to evaluate the ability to share information in real time between the 51st CST (using smartphones running MCAP clients) and Michigan's St. Clair County (SCC) Emergency Operations Center (using a GIS system called Resilient). As part of the joint exercise, real-time location of Guard members was published as a KML feed from the MCAP cloud to the SCC Resilient System. The Resilient System allows electronic white boarding, output of which was pushed to the smartphones from the MCAP cloud.

The joint exercise demonstrated MCAP's potential to push real-time information into back-end systems which traditionally have relied on manual or 'phoned-in' inputs. Exercise planners deemed the MCAP-Resilient information sharing as one of the top three things that worked well. While challenges remain for use of map work products in exchanging real-time location data, broadly speaking sharing of data using some standards driven XML work products eases integration and enables policy based sharing of data.

Acknowledgment

The MCAP investigation team acknowledges the leadership and help provided by BG Michael McDaniel, BG Michael Stone, and COL (Ret.) Keith Bobenmoyer of the Michigan National Guard.

References

[1] "Planning Scenarios: Executive Summaries," The Homeland Security Council and the Department of Homeland Security, Version 2.0, July 2004.

[2] DARPA-NS-09-20 Request for Information (RFI): Technologies for the Applications of Social Computing (TASC).

[3] Humanitarian Assistance/Disaster Relief (HA/DR) "As-Is" Model : Presentation given by Keith Holcomb, BGen, USMC (Ret) and Jack Thorpe, Col, USAF (Ret), DARPA Workshop on Strategic Collaboration, June 20, 2007, Arlington, VA.

[4] J.W. Morentz, "Unified Incident Command and Decision Support (UICDS): A Department of Homeland Security Initiative in Information Sharing," IEEE Conference on Technologies for Homeland Security, May 12-13, 2008, Waltham, MA

[5] OSGi Service Platform Core Specification Release 4. http://www.osgi.org/Specifications/HomePage

[6] OpenGIS Locatio nService (OpenLS) Implementation Specification: Core Services 1.2.0. http://www.opengeospatial.org/standards/ols

[7] OpenID Authentication 2.0. http://openid.net/developers/specs/

[8] The OAuth 1.0 Protocol. http://tools.ietf.org/html/rfc5849